EXAMINER'S AMENDMENT

1.   An examiner's amendment to the record appears below. Should the changes and/or additions be

unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure

consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Elise R.

Heilbrunn on December 22, 2008.

The application has been amended as follows:

IN THE CLAIMS:

Please see attached.

2.   The following is an examiner's statement of reasons for allowance: The prior art does not teach

nor render obvious each and every limitation of the claimed invention. Specifically, the prior art fails to

teach an performing layer 2 authentication of the Mobile Node or receiving a packet indicating that layer 2

authentication of the Mobile Node has bee performed and generating an orphaned host object including

the layer 2 information wherein the orphaned host object is generated after layer 2 authentication of the

Mobile Node has been performed, unorphaning the orphaned host object wherein the IP address

associated with the layer 2 information is received without performing layer 3 authentication of the Mobile

Node, thereby enabling layer 3 policies to be enforced without performing layer 3 authentication of the

Mobile Node.

Any comments considered necessary by applicant must be submitted no later than the payment

of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such

submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should

be directed to PHILIP J. CHEA whose telephone number is (571)272-3951. The examiner can normally

be reached on M-F 6:30-4:00 (1st Friday Off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on 571-272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Philip J Chea
Examiner
Art Unit 2453

/Philip J Chea/
Examiner, Art Unit 2453
12/23/08

/ARIO ETIENNE/
Supervisory Patent Examiner, Art Unit 2457

1.   (Previously Presented) A method for performing layer 2 authentication of a Mobile Node

supporting Mobile IP in an SSG-based network, comprising:

        obtaining layer 2 information including at least one of a MAC address or a username associated

with the Mobile Node;

        performing layer 2 authentication of the Mobile Node or receiving a packet indicating that layer 2

authentication of the Mobile Node has been performed;

        generating an orphaned host object including the layer 2 information, wherein the orphaned host

object is generated after layer 2 authentication of the Mobile Node has been performed;

        unorphaning the orphaned host object by a network device in the SSG-based network when an IP

address associated with the layer 2 information is received such that the unorphaned host object includes

the IP address and the layer 2 information, wherein the IP address associated with the layer 2 information

is received without performing layer 3 authentication of the Mobile Node, thereby enabling layer 3 policies

to be enforced without performing layer 3 authentication of the Mobile Node; and

        providing access to services based upon the IP address of the unorphaned host object.

2.   (Original)   The method as recited in claim 1, further comprising:

        obtaining a username associated with the Mobile Node;

        wherein the orphaned host object includes the username associated with the Mobile Node.

3.   (Original)   The method as recited in claim 1, wherein obtaining layer 2 information

comprises:

        receiving the layer 2 information in an access request packet;

        wherein generating the orphaned host object is performed when an access accept packet is

received indicating the Mobile Node associated with the layer 2 information has been authenticated by a

AAA server.

4.   (Original)   The method as recited in claim 1, wherein unorphaning the orphaned host object comprises:

receiving a packet including the IP address and the layer 2 information; and

updating the orphaned host object to include the IP address, thereby generating an unorphaned host object.

5.   (Original)   The method as recited in claim 4, wherein receiving a packet including the IP address and the layer 2 information comprises:

receiving an ACCT start packet including the IP address and the layer 2 information.

6.   (Original)   The method as recited in claim 5, further comprising:

receiving an ACCT stop packet including the IP address; and

deleting the unorphaned host object when the ACCT stop packet is received.

7.   (Original)   The method as recited in claim 1, further comprising:

deleting the unorphaned host object.

8.   (Original)   The method as recited in claim 7, further comprising:

receiving an ACCT stop packet including the IP address;

wherein deleting the unorphaned host object is performed when the ACCT stop packet is received.

9.   (Original)   The method as recited in claim 4, wherein the packet including the IP address and layer 2 information further includes an IP address of a network device from which the packet was received, the method further comprising:

maintaining a mapping between the IP address of the network device and the IP address of the

Mobile Node such that a mapping of one or more Mobile Nodes supported by the network device is

maintained.

10.   (Original)   The method as recited in claim 9, wherein the packet including the IP address

and the layer 2 information is an ACCT start packet.

11.   (Original)   The method as recited in claim 9, further comprising:

receiving a packet including the IP address of the network device that indicates that the network

device is not functioning; and

deleting an unorphaned host object or orphaning a host object for each of the Mobile Nodes

supported by the network device.

12.   (Original)   The method as recited in claim 11, wherein the packet including the IP address

of the network device that indicates that the network device is not functioning is an ACCT-OFF packet.

13.   (Original)   The method as recited in claim 11, wherein the packet including the IP address

of the network device that indicates that the network device is not functioning is an ACCT-ON packet.

14.   (Currently Amended)   A machine-readable computer-readable medium storing thereon

program computer-readable instructions for performing layer 2 authentication of a Mobile Node

supporting Mobile IP in an SSG-based network, comprising:

instructions for obtaining layer 2 information including at least one of a MAC address or a

username associated with the Mobile Node;

instructions for generating an orphaned host object including the layer 2 information, wherein the

orphaned host object is generated when layer 2 authentication of the Mobile Node has been successfully

performed; and

instructions for unorphaning the orphaned host object when an IP address associated with the

layer 2 information is received such that the unorphaned host object includes the IP address and the layer

2 information, wherein the IP address associated with the layer 2 information is received without

performing layer 3 authentication of the Mobile Node, thereby enabling layer 3 policies to be enforced

without performing layer 3 authentication of the Mobile Node, wherein unorphaning the orphaned host

object is performed without receiving information from a user via the SSG-based network.

15.   (Currently Amended)   An apparatus for performing layer 2 authentication of a Mobile Node

supporting Mobile IP in an SSG-based network, comprising:

       a processor: and

       means for obtaining layer 2 information including at least one of a MAC address or a username

associated with the Mobile Node;

       means for performing layer 2 authentication of the Mobile Node using at least a portion of the

layer 2 information or receiving a packet indicating that layer 2 authentication of the Mobile Node has

been performed;

       means for generating an orphaned host object including the layer 2 information, wherein the

orphaned host object is generated when layer 2 authentication of the Mobile Node has been performed;

and

       means for unorphaning the orphaned host object when an IP address associated with the layer 2

information is received such that the unorphaned host object includes the IP address and the layer 2

information, wherein the IP address associated with the layer 2 information is received without performing

layer 3 authentication of the Mobile Node, thereby enabling layer 3 policies to be enforced without

performing layer 3 authentication of the Mobile Node, wherein unorphaning the orphaned host object is

performed without receiving login information from a user via the SSG-based network.

16.   (Previously Presented) An apparatus for performing layer 2 authentication of a Mobile Node

supporting Mobile IP in an SSG-based network, comprising:

a processor; and

a memory, at least one of the processor or the memory being adapted for:

obtaining layer 2 information including at least one of a MAC address or a username associated with the Mobile Node;

performing layer 2 authentication of the Mobile Node using at least a portion of the layer 2 information or receiving a packet indicating that layer 2 authentication of the Mobile Node has been performed;

generating an orphaned host object including the layer 2 information, wherein the orphaned host object is generated when layer 2 authentication of the Mobile Node has been performed; and

unorphaning the orphaned host object when an IP address associated with the layer 2 information is received such that the unorphaned host object includes the IP address and the layer 2 information, wherein the IP address associated with the layer 2 information is received without performing layer 3 authentication of the Mobile Node, thereby enabling layer 3 policies to be enforced without performing layer 3 authentication of the Mobile Node, wherein unorphaning the orphaned host object is performed without receiving login information from a user via the SSG-based network.

17.   (Previously Presented) The apparatus as recited in claim 16, at least one of the processor or the memory being further adapted for:

enforcing layer 3 policies based upon the layer 2 authentication of the Mobile Node.

18.   (Previously Presented) The apparatus as recited in claim 16, at least one of the processor or the memory being further adapted for:

enforcing layer 3 policies without performing layer 3 authentication.

19.   (Previously Presented) The apparatus as recited in claim 16, at least one of the processor or the memory being further adapted for:

enforcing layer 3 policies by accessing the unorphaned host object.

20.   (Previously Presented) The apparatus as recited in claim 16, at least one of the processor or the memory being further adapted for:

      enforcing layer 3 policies based upon the IP address of the unorphaned host object.

21.   (Cancelled)

22.   (Previously Presented) The method as recited in claim 1, wherein performing Layer 2 authentication of the Mobile Node is performed using an EAP-SIM protocol.

23.   (Previously Presented) The method as recited in claim 1, wherein layer 2 authentication of the Mobile Node is performed using a LEAP protocol.

24.   (Previously Presented) The apparatus as recited in claim 16, wherein layer 2 authentication of the Mobile Node is performed using an EAP-SIM protocol.